Supreme Court, U.S.
MOTION FILED
NOV 14 2008
William K. Suter, Clerk

111 (3)

No. 08-500

In the

Supreme Court of the United States

CYNTHIA LAMBERT,

Petitioner,

v.

GREG HARTMANN, Clerk of Courts for Hamilton County, and HAMILTON COUNTY BOARD OF COUNTY COMMISSIONERS,

Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

---

CONSUMER ACTION AND PRIVACY RIGHTS CLEARINGHOUSE'S MOTION FOR LEAVE TO FILE AND BRIEF AS *AMICI CURIAE* IN SUPPORT OF THE PETITION FOR CERTIORARI

Eric G. Barber
Counsel of Record
PERKINS COIE LLP
One East Main St., Suite 201
Madison, WI 53703-5118
608.663.7460
Attorney for Consumer Action and Privacy Rights Clearinghouse

TABLE OF CONTENTS

Page

MOTION FOR LEAVE TO FILE AND STATEMENT OF INTEREST 1

SUMMARY OF ARGUMENT 2

ARGUMENT 3

I. The Circuits Require Guidance to Resolve a Significant Split 3

II. State And Local Government Disclosures of Confidential Information Are a Serious Problem 4

CONCLUSION 10

TABLE OF AUTHORITIES

Page

CASES

Alexander v. Peffer,
993 F.2d 1348 (8th Cir. 1993) 3

Denius v. Dunlap,
209 F.3d 944 (7th Cir. 2000) 3

Doe v. City of New York,
15 F.3d 264 (2d Cir. 1994) 3

Fraternal Order of Police v. City of Philadelphia,
812 F.2d 105 (3d Cir. 1987) 3

Greidinger v. Davis,
988 F.2d 1344 (4th Cir. 1993) 6

James v. City of Douglas,
941 F.2d 1539 (11th Cir. 1991) 3

Sheets v. Salt Lake County,
45 F.3d 1383 (10th Cir. 1995) 3

Tucson Woman's Clinic v. Eden,
379 F.3d 531 (9th Cir. 2004) 3

Walls v. City of Petersburg,
895 F.2d 188 (4th Cir. 1990) 3

STATUTES

42 U.S.C. § 405(c)(2)(C)(vi)(II) 6

42 U.S.C. § 1983 3

OTHER AUTHORITIES

Jessica Fender, *Coloradans At Risk of ID Theft*, Denver Post (July 9, 2008) 7-8

Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data (January – December 2006)* (Feb. 2007) 5

Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data (January – December 2007)* (Feb. 2008) 5

Government Accountability Office, *Social Security Numbers Are Widely Available In Bulk And Online, But Changes to Enhance Security Are Occurring*, GAO-08-1009R (Sept. 4, 2008) 8

Jaikumar Vijayan, *Colorado State Website Reveals Social Security Numbers Of Top U.S. Executives*, CIO.com (Oct. 9, 2008) 8

Mark Niquette, *Bank data on stolen tape*, The Columbus Dispatch (June 17, 2007) 7

State Cyber Security Protection Act of 2008, S. 3460, 110th Cong., § 2 (2008) 8

Synovate, *Federal Trade Commission – 2006 Identity Theft Survey Report* (Nov. 2007) 5

MOTION FOR LEAVE TO FILE AND STATEMENT OF INTEREST[1]

Consumer Action and Privacy Rights Clearinghouse move under Rule 37.2(b) of this Court for leave to file the following *amicus* brief in support of the petition for certiorari. Consumer Action and Privacy Rights Clearinghouse file this motion because respondent Hamilton County has failed to respond to written and telephonic requests for consent to this filing.

Consumer Action is a national not-for-profit education and advocacy association devoted to protecting consumers from, among other things, the frequent crime of identity theft. Consumer Action has served consumers and sought to protect their rights nationwide for 37 years by aiding consumers in handling complaints, publishing educational materials in a variety of languages, and advocating for consumers in the media and before lawmakers. In particular, Consumer Action has sought to protect those most targeted by the unscrupulous: the disabled, those with low incomes, immigrants, and the elderly.

---

[1] No party or counsel for a party has authored or contributed monetarily to the preparation or submission of any portion of this brief. On November 4, 2008, Consumer Action and Privacy Rights Clearinghouse provided all counsel of record with timely notice of its intention to file this *amicus* brief.

Privacy Rights Clearinghouse is a nonprofit consumer organization that serves individuals nationwide through both consumer information and advocacy. Privacy Rights Clearinghouse seeks to raise consumers' awareness of how technology affects personal privacy, as well as to document and respond to consumer complaints regarding breaches of privacy. Privacy Rights Clearinghouse has advocated for consumers' privacy rights in local, state, and federal public policy proceedings, including legislative testimony, regulatory agency hearings, task forces, and study commissions. It is also listed as a resource by the United States Department of Justice on the page of that department's website devoted to identity theft.

These two organizations have a common interest in this case: that some of the largest and most important keepers of confidential information—state and local governments—recognize the harm caused by intentional disclosures of private information and that they take steps to safeguard that information.

SUMMARY OF ARGUMENT

This Court should grant review of the Sixth Circuit's decision below, reported at 510 F.3d 433, because that decision not only conflicts with other circuits' decisions and Congressional action, but also leaves millions of residents within the Sixth Circuit without a meaningful remedy when they are the victims of predictable and preventable

identity theft. Further, this is an issue of significant importance to private citizens everywhere in this country.

ARGUMENT

I. THE CIRCUITS REQUIRE GUIDANCE TO RESOLVE A SIGNIFICANT SPLIT

Had Cynthia Lambert lived almost anywhere in the country outside the area covered by the Sixth Circuit, she would have been able to maintain an action under 42 U.S.C. § 1983 for Respondent Greg Hartmann's intentional violation of her informational privacy interest. As shown in Ms. Lambert's petition, the Second, Third, Fourth, Seventh, Eighth, Ninth, Tenth, and Eleventh Circuits all apply a balancing test that does not additionally require that a "fundamental liberty interest" be implicated. *See* Pet. 10 (citing *Tucson Woman's Clinic v. Eden*, 379 F.3d 531 (9th Cir. 2004); *Alexander v. Peffer*, 993 F.2d 1348 (8th Cir. 1993); *Denius v. Dunlap*, 209 F.3d 944 (7th Cir. 2000); *Sheets v. Salt Lake County*, 45 F.3d 1383 (10th Cir. 1995); *Doe v. City of New York*, 15 F.3d 264 (2d Cir. 1994); *James v. City of Douglas*, 941 F.2d 1539 (11th Cir. 1991); *Walls v. City of Petersburg*, 895 F.2d 188 (4th Cir. 1990); and *Fraternal Order of Police v. City of Philadelphia*, 812 F.2d 105 (3d Cir. 1987)). Of the circuits that have addressed the issue, only the Sixth would without question deny Ms. Lambert recourse.

The split is especially significant because the circuits that disagree with the Sixth Circuit have also developed a variety of balancing tests for determining when someone's privacy rights have been violated. Pet. 12-14. Moreover, while the circuits' confusion alone would justify granting the petition, the type of data disclosure that happened here is a problem of significant proportions.

II. State and Local Government Disclosures of Confidential Information Are a Serious Problem

Good name in man and woman, dear my lord,

Is the immediate jewel of their souls:

Who steals my purse steals trash; 'tis something, nothing;

But he that filches from me my good name

Robs me of that which not enriches him

And makes me poor indeed.

William Shakespeare, Othello, act 3, sc. 3.

Identity theft allows the thief to have both the purse and the victim's good name, enriching the thief while impoverishing the victim. Aware of this, citizens are increasingly alert to the methods of identity theft and the devastating harms that result, and they have started to protect their confidential information accordingly. They do not, however, expect their own state and local governments to scuttle those safeguards by

disclosing the information they have sought to protect (and indeed that Congress has sought to protect).

There can be no doubt that identity theft continues to be a serious problem in this country. According to one recent study for the Federal Trade Commission ("FTC"), recent years have seen over 8.3 million adults in the United States become the victims of some form of identity theft, and the cost of those thefts is measured in the billions of dollars per year. Synovate, *Federal Trade Commission – 2006 Identity Theft Survey Report* (Nov. 2007). Consumer organizations deal with the messy aftermath of such identity theft every day. "Consumer Sentinel," the FTC's complaint database, indicates that for eight years in a row, identity theft is the issue about which consumers complain most often. In 2006 and 2007, well over 30% of all complaints related to identity theft. Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data (January—December 2007)*, at 3 (Feb. 2008); Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data (January—December 2006)*, at 3 (Feb. 2007). The next most frequently complained-about type of fraud is related to shop-at-home/catalog sales and constituted only about 7% of all complaints.

The dishonest do not need much more than a Social Security number to steal someone's identity. As the Fourth Circuit put it:

> [A]rmed with one's [Social Security number], an unscrupulous individual could obtain a person's welfare benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain a person's paycheck .... Succinctly stated, the harm that can be inflicted from the disclosure of a [Social Security number] to an unscrupulous individual is alarming and potentially financially ruinous.

Greidinger v. Davis, 988 F.2d 1344, 1354 (4th Cir. 1993).

Congress spoke to this concern when it passed the Intelligence Reform and Terrorism Prevention Act of 2004, which prevents states from listing citizens' Social Security numbers on drivers' licenses and state-issued identification cards. 42 U.S.C. § 405(c)(2)(C)(vi)(II). Here, however, the Hamilton County clerk provided much more when he publicly posted Ms. Lambert's name, address, date of birth, signature, *and* Social Security number for all (including thieves) to see and abuse.

Undoubtedly, some instances of identity theft are preventable. There is no shortage of websites and organizations—including that of the Consumer Action and Privacy Rights Clearinghouse—with the specific goal of reducing identity theft. But citizens,

diligent or otherwise, do not expect that their state and local governments will needlessly and intentionally disclose the information that they have sought to protect.

Sadly though, state and local governments do disclose consumers' private data. In the first three quarters of 2008, state and local governments exposed the confidential information of 3.8 million Americans. So while the federal government has become increasingly diligent in protecting citizens' confidential information, the same cannot be said of state and local governments. Indeed, breaches by state and local governments far outnumber breaches reported by federal agencies. In 2007, for example, the State of Ohio carelessly allowed the disclosure of the names and bank data of almost all its state employees and 125,000 other individuals when an unencrypted tape containing the data was taken from an intern's car. Mark Niquette, *Bank data on stolen tape*, The Columbus Dispatch (June 17, 2007).

Ohio is not alone.[2] This year Colorado has had a poor record at preventing confidential data from appearing on state websites. On July 10, 2008, the state Department of Motor Vehicles improperly allowed access to the Social Security numbers, addresses, and other personal information of 3.4 million Coloradans. Jessica Fender, *DMV puts*

---

[2] Privacy Rights Clearinghouse maintains a database listing data breaches from 2005 to present at http://www.privacyrights.org/ar/ChronDataBreaches.htm.

Coloradans at risk of ID theft, Denver Post (July 9, 2008), http://origin.denverpost.com/headlines/ci_9822063. And just last month, Computerworld magazine discovered that the private data of executives at some of the country's largest companies, including Fortune 100 companies, were available on the Colorado Secretary of State's website. One of the documents provided the Social Security numbers, home addresses, and dates of birth of 93 top officers of a well-known financial corporation. Jaikumar Vijayan, *Colorado State Website Reveals Social Security Numbers of Top U.S. Executives* (Oct. 9, 2008), http://www.cio.com/453690/Colorado_State_Website_Reveals_Social_Secutiry_Numbers_Of_Top_U.S._Executives.

The problem of state and local government disclosure is so pervasive that Senator Norman Coleman of Minnesota recently introduced legislation that would allocate $25 million to determine how better state governments can safeguard personal data, including Social Security numbers. *See* State Cyber Security Protection Act of 2008, S. 3460, 110th Cong., § 2 (2008). Even more recently, the Government Accountability Office found that the practice of putting Social Security numbers online is common, occurring in roughly 85% of the largest counties around the country. *See* Government Accountability Office, *Social Security Numbers Are Widely Available in Bulk and Online, but Changes to Enhance Security Are Occurring*, GAO-08-1009R, at 1 (Sept. 4, 2008).

Many improvements in security are prospective only, however, leaving hundreds of thousands or millions of Social Security numbers online.

All of this demonstrates that what happened in Hamilton County in this case is not unique. Five or ten years ago experts predicted that as more personal information became available online, the need to protect such information would increase. That time is here—yet data and personal information are routinely posted online and exposed to the unscrupulous. Innocent citizens such as Petitioner no longer just face a theoretical risk of identity theft; they actually become the victims of identity theft. As the financial and credit crisis in this country becomes more acute, it will be more important for individuals to have control over their financial well-being. Even in the most stable times, identity thefts resulting from state and local government disclosures are individually destabilizing events. If state and local governments continue to disclose their citizens' confidential data with impunity, events that were destabilizing to individuals may become another factor further destabilizing an already shaky credit-driven economy. Put simply, this is an issue whose time has come.

Of course, not all disclosures of personal identifying information are actionable under Section 1983, but this case illustrates the problem resulting from intentional disclosures. The county clerk here left confidential personal information

online for months, giving would-be-defrauders plenty of time to sift through the information and identify the most vulnerable targets. Absent remedies for intentional disclosures, states and local governments may have little motivation to properly protect their citizens' confidential information.

CONCLUSION

Allowing the Sixth Circuit's decision to stand leaves millions of Americans in that circuit unprotected and at a greater risk of identity theft as compared to their fellow citizens. This Court should resolve whether Section 1983 provides an effective remedy so that more victims like Ms. Lambert are not created at the hands of the governmental bodies that are supposed to protect them.

The petition for a writ of *certiorari* should be granted.

RESPECTFULLY SUBMITTED this 14th day of November, 2008.

Eric G. Barber
Counsel of Record
PERKINS COIE LLP
One East Main St., Suite 201
Madison, WI 53703-5118
608.663.7460
Attorney for Consumer Action and Privacy Rights Clearinghouse